

18 OCT 2004

EP04106216

**PRIORITY  
DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)



REC'D 25 NOV 2004	
WIPO	PCT

**Prioritätsbescheinigung über die Einreichung  
einer Patentanmeldung**

**Aktenzeichen:** 103 26 665.8

**Anmeldetag:** 11. Juni 2003

**Anmelder/Inhaber:** Endress + Hauser Process Solutions AG,  
Reinach/CH

**Bezeichnung:** Verfahren zum Überwachen eines  
Feldgerätes

**IPC:** G 01 D, G 01 F, G 05 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 07. Oktober 2004  
Deutsches Patent- und Markenamt  
Der Präsident  
Im Auftrag

Remus

### **Verfahren zum Überwachen eines Feldgerätes**

Die Erfindung betrifft ein Verfahren zum Überwachen eines Feldgerätes gemäß dem Oberbegriff des Anspruchs 1.

5

In der Prozessautomatisierungstechnik werden vielfach Feldgeräte eingesetzt, die zur Erfassung und/oder Beeinflussung von Prozessvariablen dienen. Beispiele für derartige Feldgeräte sind Füllstandsmessgeräte, Massedurchflussmessgeräte, Druck- und Temperaturmessgeräte, pH-Redoxpotential-Messgeräte, Leitfähigkeitsmessgeräte etc., die als Sensoren die entsprechenden Prozessvariablen Füllstand, Durchfluss, Druck, Temperatur, pH-Wert bzw. Leitfähigkeitswert erfassen.

15

Neben solchen Messgeräten sind auch Systeme bekannt, die neben der Messwerterfassung auch weitere Aufgaben erfüllen; zu nennen sind hier Elektrodenreinigungssysteme, Kalibriersysteme sowie Probenehmer.

Ebenfalls als Feldgeräte werden Ein-/Ausgabeeinheiten sogenannte Remote I/Os bezeichnet.

20

Zur Beeinflussung von Prozessvariablen dienen sogenannte Aktoren z. B. Ventile, die den Durchfluss einer Flüssigkeit in einem Rohrleitungsabschnitt Steuern oder Pumpen, die den Füllstand in einem Behälter beeinflussen.

25

Eine Vielzahl solcher Feldgeräte wird von der Firma Endress + Hauser® hergestellt und vertrieben.

30

Häufig sind Feldgeräte in einer modernen Fabrikationsanlage über ein Feldbussystem (Profibus®, Foundation®-Fieldbus, HART®, etc.) mit übergeordneten Einheiten z. B. Leitsystemen bzw. Steuereinheiten verbunden. Diese übergeordneten Einheiten dienen zur Prozesssteuerung, Prozessvisualisierung, Prozessüberwachung sowie zur Bedienung und Überwachung der Feldgeräte.

Von den übergeordneten Einheiten sind auch Kommunikationsverbindungen zu weiteren Firmennetzwerken möglich.

Zur Bedienung der Feldgeräte sind entsprechende Bedienprogramme (Bedientools) im Leitsystem bzw. in der Steuereinheit notwendig. Diese Bedienprogramme können eigenständig ablaufen oder aber auch in Leitsystem-Anwendungen integriert sein.

Die Sensoren liefern Messwerte, die dem aktuellen Wert der erfassten Prozessvariable entsprechen. Diese Messwerte werden an eine Steuereinheit z. B. SPS (Speicherprogrammierbare Steuerung) weitergeleitet.

In der Regel erfolgt die Prozesssteuerung von der Steuereinheit, wo die Messwerte verschiedener Feldgeräte ausgewertet werden und aufgrund der Auswertung Steuersignale für die entsprechenden Aktoren erzeugt werden. Neben der reinen Messwertübertragung können Feldgeräte auch zusätzliche Informationen (Diagnose, Status, etc.) übertragen. Die Parametrierung und Konfigurierung der Feldgeräte erfolgt ebenfalls über das Feldbussystem.

Das Feldbussystem bezeichnet man auch als Prozesskontrollsystem.

Die Sicherheitsanforderungen an Prozesskontrollsysteme werden immer strenger. Deshalb sind in vielen Unternehmen Prozesskontrollsysteme von anderen Firmennetzwerken (SAP, Business) streng getrennt. Dadurch sollen unerlaubte Zugriffe auf Feldgeräte vermeiden werden. Momentan konzentrieren sich die Anstrengungen im Hinblick auf Sicherheit bei Prozesskontrollsystemen auf die Netzwerk-Ebene.

Zur Vermeidung von firmenfremden Eingriffen werden sogenannte Firewalls eingesetzt. Neben firmenfremden Eingriffen sind aber unberechtigte firmeninterne Eingriffe ebenso gefährlich. Bei firmeninternen Eingriffen können z. B. Parameter in Feldgeräten geändert werden oder die gesamte Kontrollstrategie geändert werden. Dies kann zu unerwünschten Änderungen im Produktionsablauf führen.

Eine Kontrollstrategie kann z. B. mit dem System FieldCare® von der Firma Endress + Hauser erzeugt werden und in die Feldgeräte geladen werden.

5 Programme, die die Parametrierung, Konfigurierung und eine Veränderung der Kontrollstrategie ermöglichen (SCADA-Systeme oder Configuration Tools) sind meist mit einem Passwortschutz ausgestattet. Hierbei ist auch eine Authorisierung der Personen die Änderungen durchführen notwendig.

10 Z. B. können bei dem Centum CS 1000 Prozesskontrollsystem von Yokogawa kritische Funktionsblöcke, die z.B. in Feldgeräten ablaufen, nur über die Eingabe von zwei Passwörtern verschiedener Personen geändert werden.

15 Bei der Firma Endress + Hauser gibt es ein Sicherheitsschutz gegen unberechtigtes Ändern von Parametern bei Feldgeräten über eine Verriegelung. Die Person, die Änderung vornehmen möchte, muss am Feldgerät einen Code eingeben bevor Änderungen am Feldgerät möglich werden.

20 Feldgeräte, die in Prozesskontrollsystemen eingesetzt werden, weisen normalerweise Mikroprozessoren mit entsprechenden Peripherie Bausteinen auf.

25 Deshalb kann aber nicht ausgeschlossen werden, dass Hardware bzw. Software oder auch deren Teile in einem Feldgerät unberechtigt ausgetauscht bzw. verändert werden. Ein derartiger Manipulation würde von einem Prozessleitsystem aus nicht erkannt werden. Sie bedeuten aber ein erheblichen Eingriff in den Prozessablauf bzw. die Kontrollstrategie.

Insbesondere auch aus gesetzlichen bzw. vorschriftsmäßigen Gründen ist es für einen Anlagebetreiber wichtig, dass ein manipulationssicheren Prozessablauf gewährleistet wird.

Aufgabe der Erfindung ist es deshalb, ein Verfahren zum Überwachen von Feldgeräten anzugeben, das ein unberechtigtes Manipulieren von Feldgeräten nicht ermöglicht.

- 5    Gelöst wird diese Aufgabe durch die in Anspruch 1 angegebenen Merkmale. Vorteilhafte Weiterentwicklungen der Erfindung sind in den Unteransprüchen angegeben.

Wesentliche Idee der Erfindung ist es, dass eine Steuereinheit, die über ein Feldbus mit dem Feldgerät verbunden ist, in zeitlichen Abständen eine individuelle Kennung des Feldgerätes anfordert und diese mit einer in der Steuereinheit abgespeicherten Kennung vergleicht. Durch diese Abfrage wird ein Austausch der Hardware bzw. der Software oder deren Teile sofort bemerkt. Insbesondere im Hinblick auf die Validierbarkeit einer Anlage ist das erfindungsgemäße Verfahren wesentlich.

15

In einfacher Weise kann es sich bei der individuellen Kennung um die Seriennummer des Feldgerätes handeln.

In einer alternativen Ausgestaltung der Erfindung kann es sich bei der individuellen Kennung um ein Schlüssel in der Gerätefirmenware des Feldgerätes handeln.

20

Denkbar ist auch als individuelle Kennung eine im Feldgeräte abgespeicherte Prüfsumme einer Speichereinheit zu verwenden.

25

Um eine zuverlässige Protokollierung der Anlage zu ermöglichen, wird bei jeder Anfrage die angeforderte Kennung in einer Datenbank mit einem entsprechenden Zeitstempel abgespeichert.

30

Sinnvoll ist ein Abspeichern der Kennung in der Datenbank nur dann, wenn eine Änderung der Kennung festgestellt wurde.

Da eine Manipulation an einem Feldgerät dem Bedienpersonal unmittelbar mitgeteilt werden muss, wird, falls eine Änderung der Kennung eines Feldgerätes festgestellt wurde, eine Alarmmeldung oder eine Warnungsmeldung erzeugt.

Da auch betriebsbedingte Änderungen am Feldgerät vorgenommen werden müssen, sollen Alarmmeldungen oder Ereignisse nur erzeugt werden, wenn diese außerhalb spezifizierter Wartungszeiträume liegen. Oder wenn die Wartung explizit erlaubt/ geplant wurde.

5

Nachfolgend ist die Erfindung anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert.

Es zeigen:

Fig. 1 Netzwerk der Prozessautomatisierungstechnik in schematischer Darstellung.

In Fig. 1 ist ein Netzwerk der Prozessautomatisierungstechnik näher dargestellt. An einem Datenbus D1 sind mehrere Leitsysteme bzw. Steuereinheiten (Workstations WS1, WS2) die zur Prozessvisualisierung, Prozessüberwachung und zum Engineering dienen, angeschlossen. Der Datenbus D1 arbeitet z. B. nach dem HSE (High Speed Ethernet) Standard der Foundation Fieldbus. Über ein Gateway G1, das auch als Linking Device bezeichnet wird, ist der Datenbus D1 mit einem Feldbussegment SM1 verbunden. Das Feldbussegment SM1 besteht aus mehreren Feldgeräten F1, F2, F3, F4, die über einen Feldbus FB miteinander verbunden sind. Der Feldbus arbeitet z. B. nach dem Foundation® Fieldbus- Standard.

Nachfolgend ist das erfindungsgemäße Verfahren näher erläutert.

Die Steuereinheit WS1 fordert in zeitlichen Abständen eine individuelle Kennung des Feldgerätes z. B. F1 an. Aufgrund der Anfrage sendet das Feldgerät F1 seine individuelle Kennung an die Steuereinheit WS1. In der Steuereinheit WS1 wird diese individuelle Kennung mit einer in der Steuereinheit WS1 abgespeicherten individuellen Kennung verglichen. Stimmt die vom Feldgerät übertragene Kennung mit der in der Steuereinheit abgespeicherten individuellen Kennung überein, so ist sichergestellt, dass keine unberechtigten Manipulationen hinsichtlich Hard- bzw. Software am Feldgerät vorgenommen worden sind. Dadurch ist eine Validierung des Prozessablaufes möglich.

Als individuelle Kennung ist die Seriennummer des Feldgerätes F1 bzw. eine Schlüssel in der Gerätesoftware möglich. Die Steuereinheit WS1 ist mit einer externen Datenbank verbunden, in der jede Abfrage mit einem Zeitstempel protokolliert wird. Dadurch ist ein Nachweis über einen längeren Zeitraum möglich.

5

In einer alternativen Ausgestaltung der Erfindung erfolgt das Abspeichern der Datenbank nur, wenn eine Änderung der Kennung von der Steuereinheit WS1 festgestellt wurde.

In der Regel finden Wartungsarbeiten an einer Automatisierungsanlage zu genau spezifizierten Wartungszeiträumen statt. Um unnötige Alarmmeldungen zu vermeiden, werden diese nur erzeugt, wenn sie außerhalb spezifizierter Wartungszeiträume liegen.

15 Die Alarmmeldung kann an der Steuereinheit WS1 angezeigt werden oder aber auch über alternative Wege z. B. eMail, SMS und Fax an die zuständigen Stellen weitergeleitet werden.

20 In einer sehr einfachen Ausgestaltung wird in der Steuereinheit nur überwacht, ob das betreffende Feldgerät z.B. F1 mit dem Feldbus FB verbunden ist und funktionsfähig ist.

Hierfür richtet die Steuereinheit WS1 eine Anfrage an das Feldgerät F1, die eine Antwort des Feldgerätes F1 erfordert. Falls das Feldgerät nicht antwortet, wird der Ausfall in der Datenbank abgespeichert.

25

**Patentansprüche**

1. Verfahren zum Überwachen eines Feldgerätes das über einen Datenbus mit einer Steuereinheit verbunden ist, dadurch gekennzeichnet, dass die  
5 Steuereinheit in zeitlichen Abständen eine individuelle Kennung des Feldgerätes anfordert und diese mit einer in der Steuereinheit abgespeicherten Kennung vergleicht.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die individuelle Kennung die Serien-Nr. des Feldgerätes ist.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die individuelle Kennung ein Schlüssel in der Geräte-Firmware des Feldgerätes ist.
- 15 4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass die Kennung eine Prüfsumme einer Speichereinheit im Feldgerät ist.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die angeforderte Kennung in eine Datenbank mit  
20 Zeitstempel abgespeichert wird.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Abspeicherung in der Datenbank nur erfolgt, wenn eine Änderung der Kennung festgestellt wurde.
- 25 7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass bei einer Änderung der Kennung eine Alarmmeldung *oder* eine Warnmeldung erzeugt wird.
- 30 8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Alarmmeldung *oder* eine Warnmeldung nur erzeugt wird, wenn sie außerhalb spezifizierter Wartungszeiträume liegt.



9. Verfahren nach einem der vorhergehende Ansprüche, dadurch gekennzeichnet, dass die Alarmmeldung *oder* die Warnmeldung an der Steuereinheit dargestellt wird.

5 10. Verfahren nach einem der vorhergehende Ansprüche, dadurch gekennzeichnet, dass die Alarmmeldung *oder* die Warnmeldung (z.B., *eMail*, *SMS*, *Fax*) in elektronischer Form versendet wird.

11. Verfahren nach einem der vorhergehende Ansprüche, dadurch gekennzeichnet, dass die Alarmmeldungen *oder* Warnmeldungen an der Steuereinheit abrufbar sind.

12. Verfahren nach einem der vorhergehende Ansprüche, dadurch gekennzeichnet, dass die Alarmmeldungen *oder* Warnmeldungen über einen Client (z.B. *Internet Explorer*) abgerufen werden können.

15


13. Verfahren zum Überwachen eines Feldgerätes das über einen Datenbus mit einer Steuereinheit verbunden ist, dadurch gekennzeichnet, dass die Steuereinheit in zeitlichen Abständen eine Anfrage an das Feldgerät richtet, die eine Antwort des Feldgerätes erfordert und falls keine Antwort vom Feldgerät kommt, dies in einer Datenbank mit entsprechendem Zeitstempel abspeichert.

20

### **Zusammenfassung**

Bei einem Verfahren zum Überwachen eines Feldgerätes, das über ein Datenbus mit einer Steuereinheit verbunden ist, fordert die Steuereinheit den zeitlichen  
5 Abstand einer individuellen Kennung des Feldgerätes an und vergleicht diese mit einer abgespeicherten Kennung.

Fig. (1)



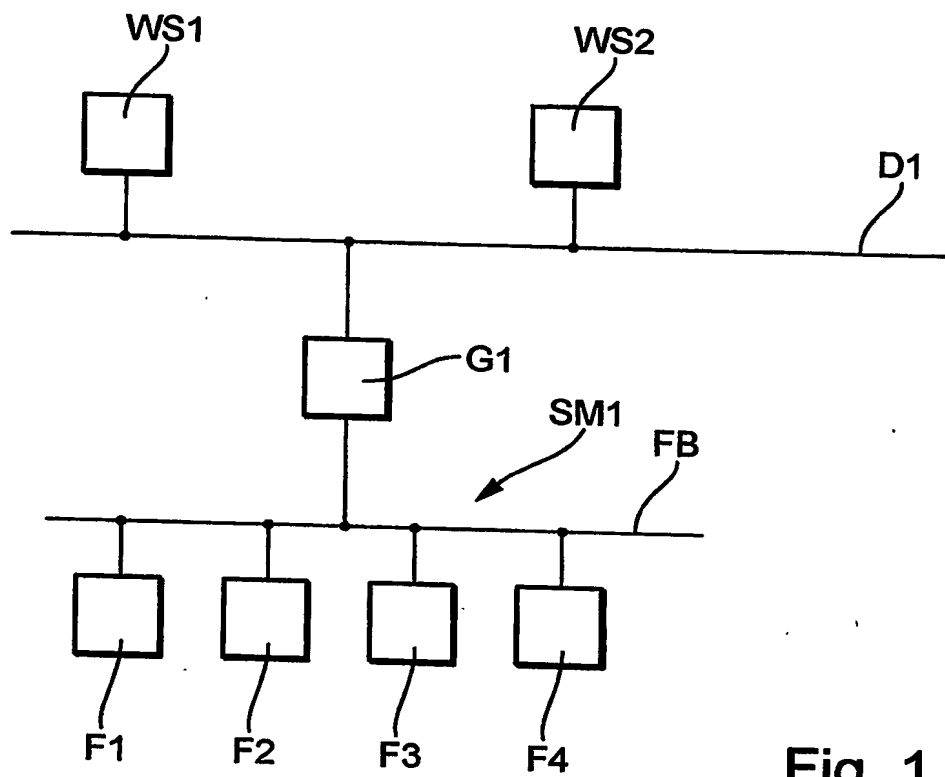


Fig. 1

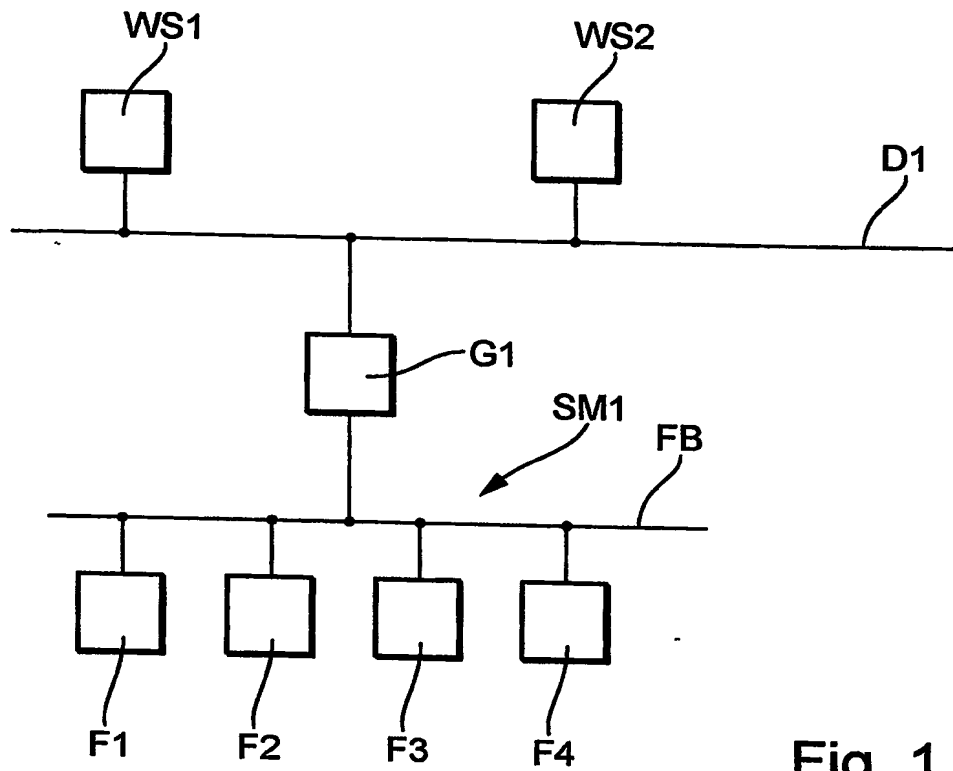


Fig. 1